Prime Divisors of Special Numbers

Author
The 2015 WOOTer

1

Introduction

In this article, we will explore some results about prime factors of numbers of the form

$$\frac{a^n - b^n}{a - b}.$$

The first chapter will consist of a review of basic facts, and in the later chapters ideas will be presented along with problems from past competitions.

There is one final note to make: p, q are understood to be primes, even though it is not stated.

2

Basic Background

2.1 Residues mod p

Define S_p to be the set $\{1, 2, ...p-1\}$ of all nonzero residues mod p.

Theorem 2.1. *For any positive integer k not divisible by p, the set $\{k, 2k, ...(p-1)k\}$ is equivalent to the set S_p when elements are taken mod p.*

Solution. Clearly $\{k, 2k, ...(p-1)k\}$ and S_p have the same number of elements. If we show each element of $\{k, 2k, ..(p-1)k\}$ is equivalent to a different element within S_p, then the proof will complete.

Assume this is not true. Then for some distinct a, b mod p, we must have $ka \equiv kb \pmod{p}$. This becomes $k(a-b) \equiv 0 \pmod{p}$ and as p does not divide k, we must have $a \equiv b$ mod p, contradiction. $\square$

Theorem 2.2. *The set $\{1^{-1}, 2^{-1}, ..(p-1)^{-1}\}$, where inverses are taken mod p, is equivalent to S_p.*

Solution. Clearly the two sets have equal magnitude, so it suffices to show that each element in $\{1^{-1}, 2^{-1}, ..(p-1)^{-1}\}$ maps to a distinct element within S_p.

To show this, assume for the sake of contradiction that two a, b distinct mod p satisfy $a^{-1} \equiv b^{-1} \equiv k \pmod{p}$ for some k. Then clearly $ka \equiv kb \equiv 1$ by the definition of an inverse. Thus, we obtain $k(a-b) \equiv 0$ but since k cannot be divisible by p, it follows that $a - b \equiv 0$, a contradiction. $\square$

2.2 Fermat's Little Theorem

Theorem 2.3 (Fermat's Little Theorem)**.** *For a not divisible by p, the relation $a^{p-1} \equiv 1 \pmod{p}$ holds.*

Solution. By Theorem 2.1, it is apparent that the set $\{a, 2a, ...(p-1)a\}$ is equivalent to S_p. Thus, the product of all the elements in each set must be equal mod p.
Then we obtain $a(2a)(3a)..((p-1)a) \equiv (1)(2)..(p-1)$ mod p. This becomes $a^{p-1} \cdot (p-1)! \equiv (p-1)!$ mod p and since $\gcd((p-1)!, p) = 1$ we obtain $a^{p-1} \equiv 1$ mod p for all a not divisible by p. $\square$

3

Primes that are $-1, 2, 3$ mod n

3.1 A New Theorem

The first new theorem that we would like to present here, which as of yet does not have a name, can be stated in three parts.

Theorem 3.1. *Suppose that* $p|\dfrac{a^n - b^n}{a-b}$ *for distinct positive integers* a, b *and some positive integer* $n > 2$. *Then the following three claims hold:*

1. *If* $p \equiv -1$ *mod* n, *then either* $p|\gcd(a,b)$ *or* $p|a+b$.
2. *If* $p \equiv 2$ *mod* n, *then* $p|\gcd(a,b)$
3. *If* $p \equiv 3$ *mod* n, *then either* $p|\gcd(a,b)$ *or* $p|a+b$

We prove the three parts separately, although the proofs are quite similar. In all three, we extensively use the fact that $a^x \equiv b^x$ *and* $a^y \equiv b^y$ *implies that* $a^{\gcd(x,y)} \equiv b^{\gcd(x,y)}$. *This is not hard at all to prove, and it is left to the reader.*

Claim 1. We note that $a^n \equiv b^n \mod p$. This follows directly from the hypothesis. Now we can write $p = kn - 1$ because $p \equiv -1 \mod n$. By Fermat's Little Theorem, we obtain $a^{kn-2} \equiv b^{kn-2} \mod p$. However, it follows from $a^n \equiv b^n$ that $a^{kn} \equiv b^{kn} \mod p$.
Putting these two equations together, it is not hard to deduce that $a^2 \equiv b^2$ or $(a+b)(a-b) \equiv 0 \mod p$. This implies $p|a+b$ or $p|a-b$. Note that we are not yet finished with what we want to prove, which is that $p|\gcd(a,b)$ or $p|a+b$.
However, suppose $p|a-b$ and then $a \equiv b \mod p$. We note that $a^{n-1} + a^{n-2}b + ... + b^{n-1} \equiv 0 \mod p$ (this follows from rewriting $\dfrac{a^n - b^n}{a-b}$) and thus by substituting $a \equiv b$ we obtain $nb^{n-1} \equiv 0 \mod p$. Since $\gcd(n,p) = 1$ it follows that $p|b$ and then $p|a$, so the claim has been proven. ☐

Claim 2. We proceed similarly but note $p = kn + 2$. By using the same steps, one may obtain the two equations $a^{kn} \equiv b^{kn} \mod p$ and $a^{kn+1} \equiv b^{kn+1}$ m
od p, where the second one follows by Fermat's Little Theorem.
Then one may deduce that $a \equiv b \mod p$ by combining the two equations. At this point, substitute $a = b$ into the equation $a^{n-1} + a^{n-2}b + .. + b^{n-1} \equiv 0 \mod p$ and we can obtain that $p|a$ and $p|b$. ☐

Claim 3. This proof is identical to that of Claim 1. There is one key difference though. We obtain $a^{-2} \equiv b^{-2}$ instead of $a^2 \equiv b^2$. However, by applying Theorem 2.2, we know that $(a^2)^{-1} \equiv (b^2)^{-1} \implies a^2 \equiv b^2$ so the result follows. ☐

3.2 Useful Corollaries of Theorem 3.1

There are two values of n where theorem 3.1 is most useful: when $n = 3$ or $n = 4$.

Corollary 3.1. Suppose $p|a^2 + ab + b^2$ where $p \equiv 2 \bmod 3$. Then $p|\gcd(a, b)$.

Solution. We apply part 2 of theorem 3.1 for $n = 3$. This is then a direct result.

Alternatively, one may apply part 1 of theorem 3.1 for $n = 3$, but then the theorem states that either $p|\gcd(a, b)$ or $p|a + b$. At this point one must root out the case where $p|a + b$ by substitution. ☐

Corollary 3.2. Suppose $p|a^2 + b^2$ where $p \equiv 3 \bmod 4$. Then $p|\gcd(a, b)$.

Solution. Applying theorem 3.1 part 1 where $n = 4$ yields that $p|\gcd(a, b)$ or $p|a + b$ where $p|\dfrac{a^4 - b^4}{a - b}$.

This is a far cry from what we wanted to prove! However, one may note

$$\frac{a^4 - b^4}{a - b} = (a + b)(a^2 + b^2)$$

. Thus, if $p|a^2 + b^2$, it follows that $p|(a + b)(a^2 + b^2)$ and then $p|\gcd(a, b)$ or $p|a + b$.

Suppose that $p|\gcd(a, b)$. Then we are done as this is what we wanted to show.

Else, suppose that $p|a + b$. Then $a^2 + b^2 \equiv 0 \bmod p$ and substituting $a \equiv -b \bmod p$ yields $b^2 \equiv 0 \bmod p$ and it follows that $p|b$. Similarly, $p|a$ so that $p|\gcd(a, b)$, which is what we wanted to prove. ☐

3.3 Example Problems

Example 3.1. *Show that there are infinitely many primes of the form $4k + 1$.*

Solution. This is very interesting.. Theorem 3.1 does not give any results concerning numbers that are 1 mod 4 (where we substitute $n = 4$).

However, we may note that all primes are either equal to 2 or are $1, 3$ mod 4.

Now assume, for the sake of contradiction, that there are only **finitely** many primes of the form $4k + 1$. We label these primes $p_1, p_2, ..p_m$. Now consider the number $N = (2p_1p_2...p_n)^2 + 1^2$.

It is evident that this number is 1 mod 4. Suppose that this number is not prime. Then it follows that it has an odd prime divisor q.

Suppose q is 1 mod 4. Then q must equal one of the p_is because $p_1, p_2, ..p_n$ is the complete list of primes which are 1 mod 4. However, it is evident for each p_i that $\gcd(N, p_i) = 1$, so it is impossible to have $q|N$.

Suppose now that q is 3 mod 4. Now it is easy to see where we are going. Apply corollary 2 of theorem 3.1 to obtain that $q|\gcd(2p_1p_2..p_n, 1) = 1$. Then this is a contradiction.

Because N is odd and has no prime factors of the form 1 mod 4 or 3 mod 4, it must be prime, and furthermore it is a prime of the form 1 mod 4. But we assumed that $p_1, p_2, ..p_n$ was the complete list of all primes which are 1 mod 4 and clearly $N > p_i$ for each i so it follows that there is a contradiction and there are infinite primes of the form 1 mod 4. ☐

Example 3.2. *Solve in positive integers the diophantine* $4ab = a + b + c^2$.

Solution. We assume there is a solution and rewrite the equation in the form $(4a-1)(4b-1) = c^2+1$. This is clearly equivalent with the original equation.

Note that $4a - 1$ is 3 mod 4. It must have a prime factor p which is 3 mod 4. (Because if this were not the case, then $4a - 1$ could not be 3 mod 4.) Then $p|c^2 + 1$ so by Corollary 2 of theorem 3, it follows that $p|\gcd(c, 1) = 1$, which is a contradiction.

Thus, there can be no positive integer solutions to the diophantine. ☐

The following problem is from the Kolmogorov Cup

Example 3.3. *Suppose there exists three positive integers* a, b, c *such that the number* $N = \dfrac{a^2 + b^2 + c^2}{ab + bc + ca}$ *is also an integer. Prove that* N *cannot be divisible by* 3.

Solution. Assume, for the sake of contradiction, that $3|N$ and write $N = 3k$. Also assume $\gcd(a, b, c) = 1$.

Then it is not hard to show $3k + 2 = \dfrac{(a + b + c)^2}{ab + bc + ca}$.

Note the left hand side must have a prime factor $p \equiv 2 \bmod 3$ such that p divides $3k + 2$ an odd number of times. (Because if this is not the case, one may prime factorize $3k + 2$ and take mod 3 to show that $2 \equiv 1$.)

However, if $p|3k + 2$ it follows that $p|(a + b + c)^2$. Now note p divides $(a + b + c)^2$ an even number of times as $(a+b+c)^2$ is a square. It follows that $p|ab+bc+ca$ (an odd number of times, but this is insignificant).

We now know $a+b+c \equiv 0$ and $ab+bc+ca \equiv 0 \bmod p$. Substitute $c = -a-b$ into the second equation to obtain $-(a^2+ab+b^2) \equiv 0 \bmod p$. However, by Corollary 1 of Theorem 3.1, we obtain $p|\gcd(a, b)$.

Similarly, we obtain $p|\gcd(b, c)$ (or by symmetry on a, b, c). It follows that $p|\gcd(a, b, c)$. However, we assumed $\gcd(a, b, c) = 1$ so we have a contradiction! ☐

Example 3.4. *Determine all positive integers* n *such that there exists a positive integer* m *with* $2^n - 1|m^2 + 9$.

Solution. Firstly, note $n = 1$ obviously works. Now assume $n > 1$. Then $2^n - 1$ is 3 mod 4 and it must have a factor that is 3 mod 4. Let this factor be p, and then $p|2^n-1|m^2+9$ so it follows that $p|\gcd(m, 3)$ and $p = 3$. We also obtain $3|m$. Then substitute $m = 3M$ so that $2^n - 1|9(M^2 + 1)$.

Now, here comes the trick: Firstly, $3|2^n - 1 \implies n$ is even. Suppose $n = 2$, then clearly this satisfies the conditions. (We can choose $m = 3$). Suppose then $n > 2$ and therefore n is composite. Write $n = 2^a \cdot b$, where b is odd.

Then $2^b - 1|2^n - 1|m^2 + 9$. Suppose $b > 1$. Then $2^b - 1$ has a prime factor which is 3 mod 4. Call it q. Then $q|m^2 + 9$ so it follows that $q|\gcd(m, 3) = 3$ by Corollary 2. But b is odd so $q \neq 3$ and we have a contradiction. It follows that $b = 1$ and $n = 2^a$.

Putting all our solutions together, n can equal $1, 2$, or 2^a. We can merge these all into one solution set: $n = 2^x$ for nonnegative x.It will be left to the reader to verify that all $n = 2^x$ work. ☐

Example 3.5. *This one is a joke. Determine all positive integers* n *such that there exists* m *with* $3^n - 1 | m^2 + 5m + 25$.

Solution. You should be able to copy all of the previous solution except use Corollary 1 instead of Corollary 2 and tweak some numbers.

Note there exists a prime $p \equiv 2 \bmod 3$ with $p | 3^n - 1 | m^2 + 5m + 25$ so Corollary 1 yields $p | \gcd(m, 5)$. Now it follows that $p = 5$ and then $5 | m$. Substitute $m = 5M$ and we obtain $3^n - 1 | 25(M^2 + M + 1)$. Now write $n = 2^a \cdot b$ where b is odd.

It follows that $3^b - 1 | 3^n - 1 | 25(M^2 + M + 1)$. Since b is odd, we cannot have $5 | 3^b - 1$. However, some prime q in the form 2 mod 3 must divide $3^b - 1$ so it follows that $q | 25(M^2 + M + 1) \implies q | M^2 + M + 1$ and Corollary 1 tells us $q | \gcd(M, 1)$, which is impossible.

Thus, there are no solutions. □

As mentioned, this final problem was a joke meant to emphasize the technique involved.

Now, one may ask, why did we only select problems involving Corollaries 1 and 2? Theorem 3.1 is a very general theorem, yet we only selected applications where $n = 3, 4$.

There are several reasons for this.

1. 3,4 are small. The advantage of this is that we can "force" the theorem to work. As seen, if $N \equiv 2 \bmod 3$, then we know there must be a prime factor of N which is 2 mod 3. If we knew $N \equiv 5 \bmod 13$, it would be very difficult to derive something significant from which the theorem could be applied.

2. Let us look at what happens when $N = 6$. Then the theorem tells us that some prime factors divide $\frac{a^6 - b^6}{a - b} = (a + b)(a^2 - ab + b^2)(a^2 + ab + b^2)$. However, we may recognize $a^2 - ab + b^2, a^2 + ab + b^2$ as factors which originate from theorem 3.1 for $n = 3$! Because $3|6$, we can see that theorem 3.1 when applied for $n = 6$ "degenerates" into theorem 3.1 applied for $n = 3$.

4

When n is prime

4.1 Theorem Statement

We mentioned in chapter 3.3 that when applying Theorem 3.1, the case of $n = 6$ basically degenerates to the case of $n = 3$, and that this occurs because $3|6$. Then, one may ask, if n is prime, this will not happen, so theorem 3 should still be quite powerful when n is prime.

Indeed, we do have a special result when when n is prime. (Remember that q is understood to be prime in this text)

Theorem 4.1. *If* $p|\dfrac{a^q-1}{a-1}$ *then either* $p = q$ *or* $p \equiv 1 \mod q$.

Proof. We note that the condition implies $a^q \equiv 1 \mod p$. We also know by Fermat's Little Theorem that $a^{p-1} \equiv 1 \mod p$. (It is impossible for $\gcd(a, p) > 1$ because $a^q \equiv 1$, so FLT is justified here.)

Combining these two relations, we can obtain $a^{\gcd(p-1,q)} \equiv 1 \mod p$.

As q is prime, either $\gcd(p-1, q) = 1, q$.

Suppose it equals 1. Then we obtain $a \equiv 1 \mod p$. Then $p|\dfrac{a^q-1}{a-1} \implies p|a^{q-1} + a^{q-2} + .. + 1$. It follows from this that $1 + 1 + ... + 1 \equiv 0 \mod p$ or $q \equiv 0 \mod p$. As p, q are prime this implies $p = q$.

Suppose the gcd equals q. Then $p - 1 \equiv 0 \mod q$ so $p \equiv 1 \mod q$ as desired. Thus, the claim is proven. ☐

Corollary 4.1. If $p = q$, then $a \equiv 1 \mod q$. If $p \equiv 1 \mod q$, then $a^q \equiv 1 \mod p$.

Proof. This follows from the proof of theorem 4. ☐

4.2 Example Problems

Example 4.1. *Show that all prime factors of* $2^p - 1$ *are greater than* p.

Solution. Note by Theorem 4.1 that $q|\dfrac{2^p-1}{2-1} \implies q = p$ or $q \equiv 1 \mod p$.

Suppose $p = q$. We obtain $2^p \equiv 1 \mod p$ but coupled with $2^{p-1} \equiv 1 \mod p$ we obtain $2 \equiv 1 \mod p$ which implies $p = 1$, impossible.

Suppose $q \equiv 1 \bmod p$ then. Either $q > p$ or $q = 1$. The second case is impossible, so we have shown all prime factors of $2^p - 1$ are $> p$. ☐

The following example is a famous result.

Example 4.2. *Show that $p^p - 1$ has at least one prime divisor of the form $1 \bmod p$.*

Solution. It is evident that the number $\dfrac{p^p-1}{p-1}$ has prime factors either equal to p or $\equiv 1 \bmod p$. The first case is ridiculous, so we consider the second one. Suppose a prime q divides $\dfrac{p^p-1}{p-1}$, then $q|p^p - 1$ and we know $q \equiv 1 \bmod p$ so the claim is proven. ☐

Indeed, this can certainly be generalized to the following statement: If a prime divisor of $p^p - 1$ does not divide $p - 1$, then it is equivalent to 1 modulo p.

The proof is identical.

For the next problem, which appeared on the Romania TST, we would like to challenge the reader to first attempt to solve it without using the ideas in this chapter. The contestants found that it was almost impossible to solve with elementary methods alone.

Example 4.3. *For a prime $p \geq 5$, show that $x^{p-1} + x^{p-2} + .. + x^2 + x + 2$ is not a perfect square.*

Solution. We note the expression is equivalent to $\frac{x^p-1}{x-1} + 1$.

Suppose this equals a square, and let it be a^2. We obtain $(a + 1)(a - 1) = \dfrac{x^p-1}{x-1}$.

Then by Theorem 4, all prime divisors of $(a + 1)(a - 1)$ are equal to p or equal to $1 \bmod p$. It is quite obvious that this is impossible. (It implies that both of $a + 1, a - 1$ have only divisors equal to p or $1 \bmod p$, and thus, $a + 1, a - 1$ simultaneously can only equal 0 or $1 \bmod p$. This is obviously impossible as $p \geq 5$). ☐

The following problem is from the 2006 ISL.

Example 4.4. *Determine all integer solutions to the equation $\dfrac{x^7-1}{x-1} = y^5 - 1$.*

Solution. We take two cases: $x \equiv 1 \bmod 7$ and x is not equivalent to $1 \bmod 7$.

In the first case, it is apparent that $\dfrac{x^7-1}{x-1} = x^6 + x^5 + .. + 1 \equiv 0 \bmod 7$. It follows that $y^5 \equiv 1 \bmod 7$ and we note that $y^6 \equiv 1 \bmod 7$ by Fermat's Little Theorem. These two facts imply $y \equiv 1 \bmod 7$.

Here comes the trick- notice that $y^5 - 1|\dfrac{x^7-1}{x-1}$ so it follows that $y^4 + y^3 + y^2 + y + 1|\dfrac{x^7-1}{x-1}$. But because $y \equiv 1 \bmod 7$, it follows that $y^4 + y^3 + y^2 + y + 1 \equiv 5 \bmod 7$. Theorem 4.1 tells us that all prime divisors of $y^4 + y^3 + .. + 1$ are $0, 1 \bmod 7$ so this is impossible and there are no solutions.

Then suppose that x is not equivalent to $1 \bmod 7$. It follows that $\dfrac{x^7-1}{x-1} \equiv 1$. Then we obtain $y^5 - 1 \equiv 1 \implies y^5 \equiv 2 \implies y \equiv 4 \bmod 7$. (The last equivalence follows from $y^5 \equiv 2$ and it is not hard to prove. One can substitute $y \equiv 0, 1, 2, 3, 4, 5, 6$ to prove it.)

But clearly $y-1|y^5-1$ and $y \equiv 4 \implies y-1 \equiv 3$ so we have just shown that there is a divisor of $\dfrac{x^7-1}{x-1}$ which is 3 mod 7. This contradicts Theorem 4, so there cannot be any solutions.

Thus, we are done, and there are no solutions in positive integers to the equation. $\square$

4.3 A Generalization

We have shown the power of theorem 4.1 using the above examples. Now, it is natural to wonder if the theorem can be generalized. It can be, but the generalization is not as useful.

Suppose a prime q divides $\dfrac{a^p-b^p}{a-b}$. Then either $q \equiv 1 \bmod p$, $p = q$, or $q|a, b$.

Proof. We proceed as in the proof of Theorem 4.1 to obtain $a^p \equiv b^p, a^{q-1} \equiv b^{q-1} \bmod q$ and it follows that $a^{\gcd(p,q-1)} = b^{\gcd(p,q-1)} \bmod q$.

Suppose that $\gcd(q-1,p) = 1$ and it follows that $a \equiv b$. Then by substituting this into the congruence $a^{p-1} + a^{p-2}b + .. + b^{p-1} \equiv 0$ we obtain $pa^{p-1} \equiv 0 \bmod q$. It follows that at least one of $p = q, q|a$ must hold. (And if $q|a$ then clearly $q|b$)

Suppose that $\gcd(q-1,p) = p$ and it follows that $q \equiv 1 \bmod p$. Note that this holds whenever $q|a^p - b^p$. $\square$

The problem with this generalization is that the case $q|a, b$ makes it remarkably weak. This makes it very hard to apply in problems, unless one is already given the condition $\gcd(a,b) = 1$ in which case it is as strong as Theorem 4.1.

Of course, there is another special case of this which is also useful. Namely, suppose b is prime. Then the generalization states that $q \equiv 1 \bmod p$, $p = q$, or $q = b$.

5

Problems for Practice

As you have now seen many applications of theorems 3.1 and 4.1, try to solve the following problems yourself.

1. In example 4 of section 3.3: We proved in the solution that all n that work must be powers of 2. Prove the converse, which is that all powers of 2 must work.
2. Find all positive integers n with $n|3^n + 1$
3. (IMO) Find all positive integers n with $n^2|2^n + 1$
4. (Bulgaria) Find all primes p, q satisfying $pq|(5^p - 2^p)(5^q - 2^q)$
5. A number N has exactly 2^{2^n} digits, all with the same non-zero value. Show that two distinct prime factors of N, say p and q, satisfy $(2^n - 1)|(p - q)$
6. (TST) Find all primes (p, q, r) with $p|q^r + 1, q|r^p + 1, r|p^q + 1$.
7. Solve in positive integers the equation $\dfrac{x^5 - 1}{x - 1} = \dfrac{y^7 - 1}{y - 1}$. This is actually significantly harder than the ISL problem we solved even though they look similar.